

CLAIMS

1. (Currently Amended) A method comprising:

determining if a smartcard is operatively available, said smartcard having smartcard memory;

requiring entry of a password and authentication by the smartcard;

identifying at least one root certificate stored in said smartcard memory;

reading said at least one root certificate from said smartcard memory;

[[and]]

storing said at least one root certificate in a computing device having computer memory operatively coupled to said smartcard, wherein the storing comprises copying said at least one root certificate from the smartcard to a certificate store maintained in said computer memory;

determining when said smartcard is no longer operatively available to the computing device; and

erasing said root certificate from said computing device when said smartcard is no longer operatively available.

2—8. (Cancelled)

Serial No.: 10/761,489
Atty Docket No.: MS1-1804US
Atty/Agent: David S. Thompson

-2-

lee & hayes The Business of IP®

www.lee-hayes.com • 509.324.9256

9. (Previously Presented) A computer readable medium having computer-implementable instructions for causing one or more processing units to perform acts comprising:

determining if a smartcard, having smartcard memory with at least one root certificate stored therein, is operatively available;

requiring user authentication for the user to discover presence of the at least one root certificate within the smartcard and to gain access to the at least one root certificate;

reading said at least one root certificate from said smartcard memory;

storing said at least one root certificate in a device operatively coupled to said smartcard, wherein said device comprises a computing device having computer memory and wherein storing said at least one root certificate in said device operatively coupled to said smartcard comprises copying said at least one root certificate from the smartcard to a certificate store maintained in said computer memory;

determining when said smartcard is no longer operatively available; and

no longer storing said root certificate in said device when said smartcard is no longer operatively available by removing said stored root certificate from a certificate store maintained in computer memory of said device by erasing it from the computer memory.

10—11. (Cancelled)

Serial No.: 10/761,489
Atty Docket No.: MS1-1804US
Atty/Agent: David S. Thompson

-3-

lee & hayes The Business of IP®

www.leehey.com • 509.324.9256

12. (Original) The computer readable medium as recited in Claim 9, having further computer-implementable instructions for causing one or more processing units to perform acts comprising:

authenticating information associated with said smartcard prior to reading said at least one root certificate.

13-16. (Cancelled)

17. (Currently Amended) A system comprising:

a computing device having computer memory;

a smartcard interface device operatively coupled to said computing device and configurable to operatively interface to a smartcard, having smartcard memory with at least one root certificate stored therein; and

~~wherein said computing device includes logic, within the computing device,~~ configured to identify when said smartcard is operatively available via said smartcard interface device, identify said root certificate in said smartcard memory, and cause said smartcard interface device to read said identified root certificate from said smartcard memory and store said root certificate to a certificate store maintained in said computer memory of the computing device; device, wherein said logic is further configured to determine when said smartcard is no longer operatively available, and remove said root certificate in said certificate store when said smartcard is no longer operatively available.

18. (Cancelled)

19. (Original) The system as recited in Claim 17, wherein said logic is further configured to authenticate information associated with said smartcard prior to causing said smartcard interface device to read said root certificate.

20. (Cancelled)**21. (Previously Presented)** A method comprising:

determining if a smartcard is operatively available, said smartcard having smartcard memory;

identifying at least one root certificate stored in said smartcard memory;

reading said at least one root certificate from said smartcard memory;

storing the at least one root certificate, by copying said at least one root certificate from the smartcard to a certificate store maintained in computer memory of a computing device operatively coupled to said smartcard;

determining when said smartcard is no longer operatively available to the computing device; and

erasing said root certificate from said computing device when said smartcard is no longer operatively available.

22. (Previously Presented) The method as recited in Claim 21, further comprising:

authenticating information associated with said smartcard prior to storing said at least one root certificate.

Serial No.: 10/761,489
Atty Docket No.: MS1-1804US
Atty/Agent: David S. Thompson

-5-

lee & hayes The Business of IP®

www.leeandhayes.com • 509.324.9256

23. (Previously Presented) A computer readable medium having computer-implementable instructions for causing one or more processing units to perform acts comprising:

determining if a smartcard is operatively available, said smartcard having smartcard memory;

reading said at least one root certificate from said smartcard memory;

storing at least one root certificate in a computing device having computer memory operatively coupled to said smartcard memory, wherein the storing comprises copying said at least one root certificate from the smartcard to a certificate store maintained in said computer memory;

determining when said smartcard is no longer operatively available to the computing device; and

erasing said root certificate from said computing device when said smartcard is no longer operatively available.

24. (Original) The computer readable medium as recited in Claim 23, having further computer-implementable instructions for causing one or more processing units to perform acts comprising:

authenticating information associated with said smartcard prior to storing said at least one root certificate in said smartcard memory.

25—33. (Cancelled)